jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 4, PP. 687-693
Manuscript received May 3, 2020; revised October, 2020. DOI: 10.24425/ijet.2020.134028

# Cryptographic Protection for Military Radio Communications

Robert Białas, Marcin Grzonkowski, and Robert Wicik

***Abstract*—Protecting the confidentiality, integrity and availability of information is very important in any telecommunications system. Information protection requires use of necessary physical, personal, information and communication technologies and above all – electromagnetic and cryptographic security measures. Equipment and tools for cryptographic protection should be examined and assessed in terms of resistance to known threats. Additional requirements are put on information protection for radio communication, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connections, bit rates are relatively low, often without full duplex. All this has an impact on the methods of cryptographic synchronization and implementation of cryptographic functions. A different approach to information protection is required by classic narrowband radio communications, a different one in time-division multi-access modes, and another one in broadband packet data transmission. Systems designed for information protection in radio communications implement appropriate operating modes of operation for cryptographic algorithms and protocols. Latest threats from quantum computers pose new challenges, especially in systems using public-key cryptography, because there are algorithms that can be used to attack these schemes with polynomial complexity.**

***Keywords*—cryptography, cryptanalysis, radio communication, quantum computers**

## I. Introduction

INFORMATION affecting security should be processed under conditions that prevent the loss of confidentiality or integrity and ensure only authorized access to it. This is especially important in radio telecommunication systems where the risks of loss information confidentiality are extremely high.

Cryptographic modules for narrowband and broadband radios have been developed for years. These projects take into account specific requirements of radio transmission in poor propagation conditions and with intentional interferences, which results in varying connectivity and low data throughputs in communication channels. The need to build advanced networks and implement a number of services are further challenges for radio communication and its security.

The latest threats from cryptanalysis methods using quantum computers have an impact on cryptographic algorithms and protocols. In the case of symmetric cryptography (with secret keys) there is a need to extend the keys, encrypted blocks, integrity and authentication tags. While, for asymmetric cryptography (with public keys) additional security mechanisms should be used at present, and in the near future new algorithms and protocols resistant to cryptanalysis performed on quantum computers should be developed and implemented.

## II. Information Protection

### A. General Requirements

Required level of security is defined depending on the classification of protected information and identified threats in the exploitation environment. There are no reduced requirements for systems operated in battlefield conditions also for systems using radio communications.

When building a cryptographic system for the protection of information, especially classified, one must take into account potential threats, specify security features, perform the design and implementation, conduct security tests, and then ensure the proper implementation for use. It is a costly process that is subject to the risk of change. Radio communication places additional requirements because of varying connectivity, no full duplex connections, channels with low data capacity, potentially long delays and optional work in radio silence.

Today, the risks of cryptanalysis using quantum computers should be taken into account. Additional security mechanisms should be implemented for currently used public-key cryptography. Symmetric cryptography algorithms should have extended keys and other parameters. All this affects communication and cryptographic protocols.

### B. Cryptography and Cryptanalysis

Cryptography and cryptanalysis are complementary parts of cryptology. Cryptography deals with methods to ensure the confidentiality, integrity and availability of information, while cryptanalysis deals with attacks that allow an adversary to break these protections.

Algorithms and protocols are an important element of any cryptographic system. Cryptographic algorithms are constructed and used to provide services such as confidentiality, integrity, authentication and non-repudiation. Cryptographic protocols are used, among others, for authentication and key agreeing. All cryptographic algorithms and protocols need cryptographic data for operating, i.e. keys, passwords, random data, identification data. The security provided by these algorithms and protocols depends largely on keeping keys secret. The security of the algorithms themselves is based on their design and the lack of effective methods of cryptanalysis.

The authors are employees of the Cryptology Department, Military Communication Institute, Zegrze, Poland (e-mail: r.bialas@wil.waw.pl; m.grzonkowski@wil.waw.pl; r.wicik@wil.waw.pl)

The selection of appropriate algorithms and protocols and their operating modes depends not only on the classification of protected information, but also on the specificity of a given system – including threats and transmission possibilities. Special cryptography modes and dedicated security profiles are often specified for radio communication. The latest threats from quantum computers also affect the selection of cryptography.

### C. *Symmetric and Asymmetric Key Material*

In symmetric cryptography the communicating parties use the identical copies of the key material, also known as pre-placed key. Symmetric key has two major disadvantages, both associated with key management. First, if any key in the communications network is compromised, all communications on that network are compromised, including past transmissions using the same net key which may have been recorded. The secret of the key must be kept until the end of its validity period. If the key secret is lost, all communicating parties must exchange the key. The second disadvantage concerns the requirement of direct key distribution. Symmetric key material must be distributing to all sites before use in a secure manner.

In cryptography using an asymmetric key material each side has a public and a private key component. Asymmetric key negotiation provides a secure communication with unique key material valid only for that session. The first step is for the two sides of the communication to exchange authentication certificates to prove to the other side that they are both valid users. After authentication, each side performs an algebraic operation to their public component, and transmits that information in the clear to the other side. Upon receipt, this public information is combined with private component to derive a unique symmetric session key. The strength of this system lies in the unique session keys as opposed to the common shared key in a symmetric pre-placed key system. Unfortunately, public-key cryptography requires a trusted third party for authentication as well as time and data consuming protocols.

### D. *Encryption Devices*

Electronic, digital encryption devices have been designed for decades for the army and special services, including those used to protect information in radio communications. Last years brought significant changes in the approach to the protection of information. We began to use standards in designing and assessing the security of cryptographic systems. Modern sets of cryptographic algorithms have been designed to meet security requirements. Efficient hardware methods for random numbers generation and complete systems for planning, generation and distribution of keys have been developed. Security requirements have forced a formal approach to tests and evaluations of cryptographic devices

The use of the newest electronic technologies, mechanical and electromagnetic security as well as newly designed cryptographic algorithms has allowed the construction of encryption devices and key management systems to successfully pass safety requirements. These include link encryptors and also devices for information protection in packet networks, generally with the Internet Protocol. Link encryption devices are used to protect information in less complex telecommunications systems using also legacy radios. IP encryptors can be used to protect information in radio networks too, if the packet data exchange is available.

Currently, research, development and implementation works are underway for crypto devices dedicated to radio transmission – narrowband and broadband also with the IP. These devices implement specific protocols for establishing encrypted connections and implementing encryption in operating modes dedicated to radio and satellite transmission.

### E. *Management of Cryptographic Keys*

An important element of any information protection system is the cryptographic key management subsystem, which is designed to meet the needs of cryptographic devices for keys and other materials necessary for their work. Such subsystems are traditionally built with several modules responsible for preparing a plan of secret connections, generating, authenticating and distributing cryptographic keys and also monitoring and management of the encrypted communication network.

Recently implemented systems automate many of these functions. Key management for the information protection in radio networks has its own specifics, hence keys loaded from electronic media directly to devices are often used to ensure their long-term operation even without radio communication with the management center. Also, establishing encrypted connections and agreeing session keys are simplified – protocols with a small number of runs and resistant to high error rates and other connectivity issues are used.

## III. Protection of Information in Military Radio Communications

In the tactical environment, communications require interoperable and flexible infrastructures to support the rapid reaction capabilities of an operational commander. The services are required within and between all levels of command. Current operational needs require interoperability of various types of telecommunications networks. The requirement for secure communications adds an additional layer of complexity to this already challenging environment.

Military radio communication is characterized by the uncertainty of establishing and maintaining connections. Even if radio devices ensure high efficiency and quality of connections, in battlefield conditions, in the presence of an enemy actively affecting radio space, this statement is highly probable. The above has an impact on cryptographic algorithms and protocols used to protect information in radio communication, their modes of operation and key management subsystems.

### A. *Narrowband Systems*

Narrowband radio communication systems are most often organized to work in HF or VHF radio networks which enable the transmission of voice signals or serial data [1]. Some radios have implemented more advanced modes of operation, e.g. TDMA or ALE. There are also those that support packet data transmission (IP), selected services such as e-mail or tracking the position of troops [2]. But many of them do not provide information protection. Therefore, we constructed crypto module as an external device, which can be attached to any type of radio, if only it provides a compatible type of communication interface. Such a common interface turned out to be a synchronous serial interface, which is made available by modems of most narrowband HF and VHF radios.

The crypto module works synchronously with the clock given from the radio – so the type and transmission speed settings are made only in the radio, and the module adapts to them. The module can be connected with terminal devices via a synchronous or asynchronous serial interface. These modules work in simplex mode – at the moment one of them encrypts data to the transmitting radio and others from the group decrypts data from receiving radios. Scheme of work of the stream encryptor and decryptor in crypto modules is presented in the Fig. 1. Data transmission is controlled by send and receive signals (RTS, CTS, etc.), which allows it to be organized in half-duplex mode. There may be more than one decryptor on the receiving side.

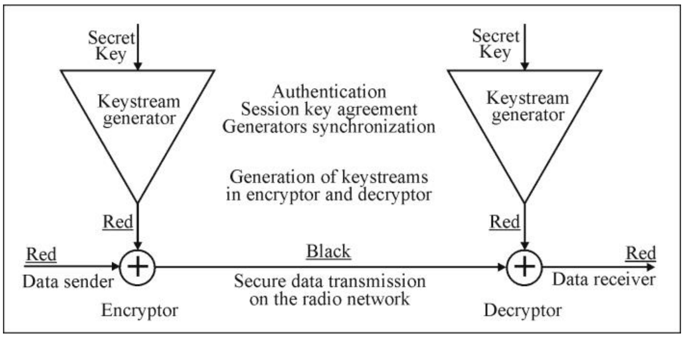

Fig. 1. Scheme of work of the stream encryptor and decryptor

Many tests have shown effective cooperation of the crypto modules with many HF and VHF radios in various operating conditions and various modes of serial transmission. The use of the module did not affect the effectiveness of establishing connections and did not degrade the quality of voice and data transmission. This was possible thanks to the use of an appropriate crypto connection protocol – setting session keys and crypto synchronization, resistant to poor transmission conditions – high error rate, as well as a cipher mode adapted to simplex or half-duplex operation, which does not duplicate any transmission errors that may occur (while the radios maintain the continuity of transmitting and receiving clocks). It was also possible to obtain secret connections between radios of different manufacturers when they work in compatible data transmission modes.

The crypto module allows encryption at speeds adapted to the mode of operation of the radio, at transmission rates from 50 bit/s to even several dozen kb/s. This is quite enough for narrowband radios. The main limitation introduced by this module is the need to separate user signals, which should be kept secret, from radio control signals that should reach the radio in an uncovered form. An additional disadvantage may be the additional delay in data and voice transmission introduced by the module.

Tests of the crypto module performed with the HF radio RKP-8100 from CTM (Centrum Techniki Morskiej, eng. Maritime Technology Center) showed its correct operation during data and voice transmission. An interesting solution used during these tests was the IZG-2000 integrator, which integrate the radio with crypto module and voice and data transmission services. Work diagram of the crypto module with the RKP-8100 radio and the IZG-2000 integrator is presented in the Fig. 2.

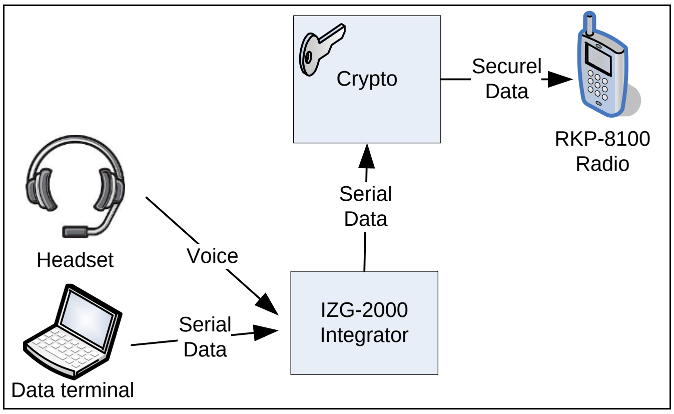

Fig. 2. Work diagram of the integrator with crypto module

IZG-2000 has a built-in MELP hardware vocoder operating at a rate of 600 bit/s. In addition, it has a serial interface for asynchronous data transmission. The integrator has a built-in priority mechanism for voice transmission. After the tangent is pressed the integrator stops sending data with the simultaneous permission to send data from the vocoder. After releasing the tangent, the integrator allows further transmission of held data from the terminal. These functionalities have been verified with the crypto module introduced in the transmission line between the integrator and the RKP-8100 radio.

### *B. Broadband Systems*

Broadband radios allow us to build more advanced communications networks in terms of organization and management, throughput available to users and support for many types of services [3]. And just, as in narrowband radios, packet transmission is rather an addition to operating modes, so in broadband radios it is a standard. Hence, the approach to cryptographic information protection for broadband radios may be closer to classic IP networks. But, the specificity and limitations of radio systems still need to be taken into account. There is no fixed communication infrastructure in a tactical environment. Networks are formed by radios that can play a role of routers or endpoints, which communicate with each other over the air, where the topology of this network changes. Some of the nodes may need to be able to operate in radio silence, where they must be able to listen in on the network, but not expose their position through transmission. So, cryptographic protocols for establishing secure connections and also encryption modes should take into account these restrictions.

Currently, broadband radios and standards implemented in them are being developed among allies. In the area of military radio communication so-called waveforms are developed defining a number of functions implemented in the radio that transform the user signals into signals emitted by the radio antenna. In addition, this type of radio has built-in intelligence enabling highly automated establishing and maintaining the appropriate quality of connections, organizing extensive wireless communication networks (also working in motion) and supporting the implementation of various services and applications for users. Examples of this type of waveforms are: ESSOR HDR (European Secure Software Defined Radio Program High Data Rate Waveform) and Coalition Wideband Networking Waveform (COALWNW).

In the area of information security, cryptographic protocols and algorithms with their operating modes and profiles specifying their use are standardized within NATO. The Secure Communications Interoperability Protocol (SCIP) standard [4] based on the American Future Narrowband Digital Terminal (FNBDT) project is dedicated to protect information transmitted over switched narrowband channels. SCIP operates at the application layer and allows establishing a secure voice connection or data transmission on a previously established duplex channel. SCIP operating on pre-placed keys (PPK) can also be used for communication on simplex radio channels and for point-to-multipoint communication. The standards for secure communication TSVCIS (Tactical Secure Voice Cryptographic Interoperability Specification) and STaC-IS (Secure Tactical Communications – Interoperability Specification) are defined for tactical radio. A version of SCIP protocol is also defined over IP, which allows its use in broadband radios, but not all required operating modes have been covered by this standard so far. That is why NATO NII IP Network Encryption (NINE) standard [5] based on the American High Assurance Internet Protocol Encryptor (HAIPE) is designed to ensure the security of IP packet communications, also using radios. NINE uses the set of IPsec protocols to provide encryption and authentication of data sent in IP networks after prior authentication and key agreement of the communicating parties.

Cryptography in radios is used to ensure transmission security (TRANSEC), security of organized networks (NETSEC) and security of transmitted user information (COMSEC). Broadband radios provide user interfaces, where in the data link layer dominates Ethernet and in the network layer – IP technology. Therefore, cryptographic solutions designed to protect information should be tailored to these technologies. The NINE standard is suitable for implementation in broadband radios based on IP packet transmission. The radio profile for NINE is being defined. Taking into account the specificity of radio communication, to the profile are chosen those operating modes that charge communication channels as little as possible, and minimize the use of a trusted third party for authenticating and use pre-placed keys to fast establish secret relationships (compared to multi-pass authentication protocols and session key agreeing using public key cryptography).

TABLE I
SCIP AND NINE COMPARISON

| | SCIP | NINE |
|---|---|---|
| Layer in model OSI | Application Layer (Layer 7) | Network Layer (Layer 3) |
| Main purpose | Voice | Data |
| Aauxiliary fate | Data | Voice |
| Throughput | 50 b/s – several Mb/s | tens kb/s – 10 Gb/s |
| Types of networks | any networks in the lower layers | IP networks |
| Develop a session key | Symmetric and asymmetric cryptography | |
| Key distribution (NATO) | Common KMI for SCIP and NINE | |

Short comparison of SCIP and NINE protocols is presented in the Table I. Key management is another important issue for secure connectivity. For SCIP and NINE standards, we can use asymmetric cryptography with public key or symmetric cryptography with secret keys. Secret keys (PPK, APPK) provided before the mission to communicating radios will allow faster and more reliable establishment of encrypted connections. This is beneficial in radio communication where there are deficits in the available bit rates. In addition, point-to-multipoint connections can be established only with secret pre-placed keys. Again, the use of public-key cryptography makes the encrypted connections more flexible, but requires a trusted third party, as well as authentication protocols and session key agreement that overload communication channels. Hence, the selection of the appropriate key management method must be preceded by an analysis to match the solution to the capabilities of radio networks as well as to the needs of users and security requirements.

## IV. KEY MANAGEMENT INFRASTRUCTURE FOR RADIO

Military radio stations should support cryptographic key management models for the two primary types of keying material, which are asymmetric and symmetric. As the infrastructure to support asymmetric key management for Radios matures in NATO, it is expected that this model will become a dominant key management approach in the future. Currently used systems use model for distribution of symmetrical keys.

### A. *KMI for Narrowband Systems*

In a typical implementation, a Key Management Infostructure (KMI) for the distribution of symmetric keying material consists of a hierarchical structure with a central node on top of the hierarchy that operates as an oversight authority and key processing facility. The central facility supervises acquisition and/or generation of keying material as well as initiates a unidirectional distribution of keying material down to the client nodes, which may in complex environments involve intermediate management tiers as well. The client nodes operate as interfaces for access to KMI functions, which include the requesting of keying material.

This solution has been implemented and tested for HF and VHF military radio stations with internal and external crypto modules.

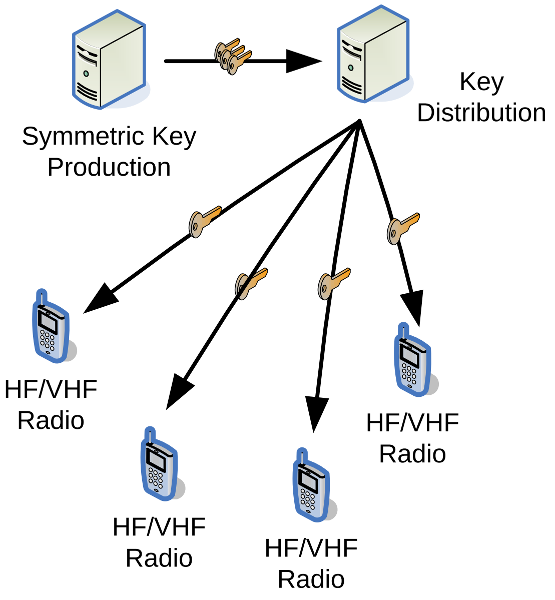

Fig. 3. KMI for narrowband radio systems

### B. *KMI for Broadband Systems - PKI*

In the future, all military radio stations should support PKI infostructure. In a typical PKI implementation, a Certification Authority (CA) plays the most important role – trusted party. A CA is a virtual entity that is trusted to create and manage public key certificates over their lifetime. A CA is bound to a certificate policy, and a certificate practice statement. CAs are supported by additional components, including:

- a repository of PKI information such as PKI certificates and Certificate Revocation Lists (CRLs), which is typically X.500 compliant with a Lightweight Directory Access Protocol (LDAP) interface;
- a suit of servers (typically Web-based) for the purposes of enrolment, certificate resigning/renewal, Online Certificate Status Protocol (OCSP) interactions, CRL distribution, certificate management messaging, CA administration, logging, etc.;
- an ECU Registration Management component, which is an optional component utilized for large and/or geographically/functionally distributed customer bases to support enrolment of users and management of issued certificates.

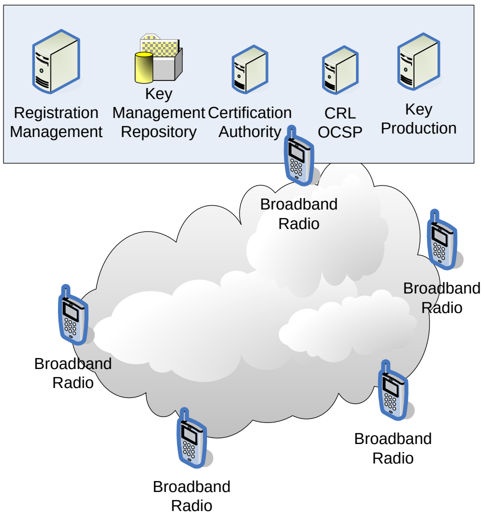

Fig 4. KMI for broadband radio systems

## V. Threats from Quantum Computers

Symmetric cryptography algorithms are used to ensure data confidentiality, integrity and authentication. These algorithms are computationally effective, and their security is based on a secret, shared cryptographic keys. Such keys must be securely delivered to users, which will challenge the subsystem for the generation and distribution of cryptographic data. Also, the flexibility (e.g. adding a new user) of symmetric key systems has some limitations.

Since the late 70s of the 20th century, we have been observing the development of asymmetric cryptography with public-private key pairs and asymmetric key agreement protocols based on public parameters. Cryptography and protocols of this type allow to provide flexibility in the operation of telecommunication systems. Subsequent system users can join secure communication when they authenticate their public keys and parameters and keep their private keys secret. Protocols for key agreement of symmetric session keys, which are then used to protect the confidentiality of transmitted data, base on public-key cryptography.

Simultaneously with the development of public-key cryptography we are observing the progress in their cryptanalysis [6]. The previously known algorithms for solving computationally difficult problems, which are behind the security of public-key cryptography, have the exponential complexity (memory or time) using classical computers to such type of the attacks. Unfortunately, using quantum computers, there are algorithms [7] that can be used to attack public-key schemes with polynomial complexity. For example, the Shor algorithm provides exponential acceleration of the factorization problem by using the superposition of quantum states. Quantum computers also have a negative impact on the security of symmetric key cryptographic algorithms [8], because the Grover algorithm [9] and Simon's algorithm [10] allow the construction of effective, quantum attacks on this type of cryptographic transformations. For the practical implementation of the algorithms of Shor, Grover, Simon, there is a lack (for now) of efficient quantum computers with an industrial scale of application.

### A. *Security Degradation of Key Agreement Protocols*

The possibility of launching an attack using a quantum computer has serious implications for the security of currently used cryptographic mechanisms applied during agreement of the session key using public-key algorithms. Asymmetric algorithms and protocols based on difficult computational problems: factorization of integers (e.g. RSA) or discrete logarithm (e.g. DH, MQV, DSA, ECDH, ECMQV, ECDSA) [11], in the model of attack using a quantum computer, they no longer provide security [12]. This is due to the fact that there are algorithms that can be performed on a quantum computer, which significantly reduce the computational complexity of cryptosystems based on these problems.

Having a quantum computer, that will be able to effectively implement the Shor algorithm, it can be stated that cryptographic algorithms based on the factorization and discrete logarithm problems will lose their significance, regardless of the length of used keys. RSA with 2048 or 4096-bit keys, DSA and DH based on Elliptic Curves with P-256, 384 or 521 – all these algorithms have polynomial security in function of the key length on quantum computer. Security degradation is due to the fact that the time needed to break these cryptosystems will be much less than the time they need to effectively perform their cryptographic functions (e.g. confidentiality of the agreed key, or digital signature security).

At present, public-key algorithms and protocols must be reinforced with private-key mechanisms. Ultimately, these algorithms must be replaced with structures resistant to attacks using quantum computers. Intensive work is ongoing in this area.

### B. *Reduction of the Security of Symmetric Algorithms*

The Grover algorithm is an implementation of searching for an element that meets certain conditions in an unordered set with $2^n$ elements. Classical algorithms require $O(2^n)$ operations, while the Grover algorithm requires only $O(\sqrt{2^n})$ operations, which gives a quadratic gain in performance on quantum computer. Let's consider a symmetric block algorithm using $n$-bit cryptographic key. Then the classical attack has the complexity of $O(2^n)$, while the attack using the Grover algorithm on a quantum computer has the complexity of $O(2^{n/2})$.

The effectiveness of the attack using the Grover algorithm does not depend on the currently used symmetric algorithm that ensures confidentiality, but only on the bit length of the cryptographic key used. Scientific analyzes indicate that in the case of symmetric algorithms ensuring confidentiality (in the context of quantum computers) security can be ensured by extending the cryptographic keys from currently used range 128÷256 to 256÷512 bits. Encrypted blocks should also be extended.

### C. Security Reduction of Cryptographic Hash Functions

The family of cryptographic hash functions is also vulnerable to a quantum attack using the Grover search algorithm. The Grover algorithm can be used to find collisions for cryptographic hash functions, with complexity being the square root of the complexity resulting from the length of the hash generated by the function, as is the case with searching a disordered database. In addition, it has been proven that it is possible to combine the Grover algorithm with the birthday paradox – we will then get a quantum birthday attack method. By creating an array of size $\sqrt[3]{2^n}$ and using the Grover algorithm to find collisions, it is possible to construct an effective quantum attack. This means that in order to provide $n$-bit security against an attack using the Grover algorithm running on a quantum computer, the cryptographic hash function must generate a $3n$ bit hash. Therefore, in order to ensure 128-bit security of the integrity of information secured using the hash function, it is necessary to use its version designating the 384-bit hash. The cryptographic functions SHA-2 and SHA-3, which determine the hash of at least 384 bits, remain secure against attacks using quantum computers.

### D. Loss of Security of Data Authentication

Data authentication modes of operation of cryptographic algorithms are designed to guarantee the authenticity of the message. The standard security model is that it is difficult to forge a message with a valid tag, even having access to the oracle, which calculates the MAC (Message Authentication Code) tag of each selected message. In order to transfer this concept of security to a quantum case, it is assumed that the opponent receives an oracle that accepts the quantum superposition of the message as input and calculates the superposition of the corresponding MAC. In the quantum attack model, the Simon's algorithm helps to solve the problem of finding $n$-bit mask for Boolean function defined over the set $\{0,1\}^n$. This problem can be solved classically by looking for a collision with the time complexity $O(2^{n/}2)$. Simon's algorithm solves this problem with only $O(n)$ quantum complexity.

The Simon's algorithm performed on a quantum computer allows an attack on the following authentication modes using symmetric algorithms as ideal permutations: CBC-MAC, PMAC, GMAC, GCM, OCB, causing the loss of authenticity of secured data. The computational complexity of the attack is only $O(n)$, where $n$ is the length in bits of the data block processed by the symmetric algorithm, and it is generally 128. Loss of authentication security in an attack model using a quantum computer immediately translates into the security problem of the set of IPsec protocols ensuring encryption and authentication of data sent in IP networks, also using the authenticated GCM encryption mode of operation. The success of the attack on the authentication mode does not depend on the currently used symmetric algorithm.

## VI. Conclusion

Building a cryptographic system, we must consider various aspects of potential threats, security features, efficiency and reliability of implementation. Equipment and systems designed for cryptographic protection of information should be examined and assessed. Additional specific requirements are put on information protection measures for radio communications, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connection, bit rates are relatively low and most often there is no full duplex. All this has an impact on implementation of cryptographic algorithms and protocols, which should use simplified operating modes. This applies in various ways to narrowband and broadband radios. Also, key management systems operating for a cryptographic protection of radio communications should not be too heavy.

We are currently facing further challenges related to information security, also in radio communications. Cryptographic algorithms are at risk from quantum computers. Symmetric algorithms ensuring confidentiality should be strengthened by extending the cryptographic keys from 256 bits up. However, this will affect their performance and probably will require an analysis of resistance to other cryptographic attacks. It is also possible to use cryptographic hash functions which are safe in the classical model, determining a hash of at least 384 bits, which remain resistant to attacks using quantum computers. Also, other secure modes of operation can be selected for data authentication that use symmetric algorithms. All this will affect the effectiveness of information protection in radio transmission.

It will probably take several years to build quantum computers useful to cryptanalysis. However asymmetric algorithms with public keys should be made today resistant to the specific properties of quantum computers, for example by using symmetric techniques with secret keys. In the near future, currently used public-key algorithms must be replaced with new ones. The U.S. NIST has initiated a process to evaluate and standardize quantum-resistant public-key cryptographic algorithms. The second round of the competition is already underway. Newly developed asymmetric algorithms, resistant to cryptanalysis using quantum computers, first of all should be used in protection systems dedicated to classified information

The above-mentioned recommendations should be implemented in the cryptographic modules being developed to protect transmitted information in radio communication systems to ensure an adequate level of security, not only today, but also in the future, when the threat from quantum computers will be real. These forces changes to many communication and cryptographic protocols, including those implemented as part of the SCIP and NINE standards and their radio profiles.

## REFERENCES

[1] M. Wiśniewski, A. Dobkowski, R. Matyszkiel, P. Kaniewski, B. Grochowina, Test results of Polish SDR narrowband radio, IEEE Communication and Information Technologies, 2017.

[2] M. Małowidzki, P. Kaniewski, R. Matyszkiel, P. Bereziński, Standard tactical services in a military disruption-tolerant network: Field tests, IEEE Military Communications Conference (MILCOM), 2017.

[3] R. Matyszkiel, P. Kaniewski, R. Polak, D. Laskowski, The results of transmission tests of polish broadband SDR radios, IEEE Communication and Information Technologies, 2017.

[4] STANAG 5068, Secure Communications Interoperability Protocol (SCIP).

[5] STANAG 4787, Network and Information Infrastructure (NII) Internet Protocol Network Encryption (NINE)

[6] M. Borowski, R. Wicik, Cryptographic protection of classified information in military radio communication faced with threats from quantum computers, Proc. SPIE. 11442, Radioelectronic Systems Conference, Jachranka, 2019.

[7] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer, SIAM Journal on Computing, Volume 26 Issue 5, 1997, p. 1484-1509.

[8] M. Kaplan, G. Laurent, A. Leverrier, M. Naya-Plasencia, Breaking symmetric cryptosystems using quantum period finding, Advances in Cryptology – CRYPTO 2016, LNCS vol. 9815, Springer, 2016.

[9] L. K. Grover, A fast quantum mechanical algorithm for database search, Bell Labs, 1996.

[10] D. R. Simon, On the Power of Quantum Computation, SIAM Journal on Computing, Volume 26, Issue 5, 1997

[11] P. Dąbrowski, R. Gliwa, J. Szmidt, R. Wicik, Generation and Implementation of Cryptographically Strong Elliptic Curves, Number Theory Methods in Cryptology (NuTMiC), Warszawa, LNCS 10737, 2017, p. 25-36.

[12] M. Borowski, J. Gocałek, R. Wicik, Securing the session key agreement protocol against cryptanalysis using quantum computers, Polish: Zabezpieczenia protokołu uzgadniania kluczy sesji przed kryptoanalizą przy wykorzystaniu komputerów kwantowych, KSTiT, Wrocław, Przegląd Telekomunikacyjny nr 7/2019.